**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software
   1. What are the two types of modern encryption methods?

The two types of modern encryption are the symmetric-key encryption and the asymmetric-key encryption. Symmetric-key encryption works with both the sender and the receiver having the same shared key installed on their computer. Asymmetric-key encryption is somewhat different it works on the basis of two keys, one is public and one is private. The public key is given by your computer to any computer that wants to communicate securely with it, the private key will only be known to your computer.

1. Network policies, profiles

Network profiles and policies are created by the administrator of a certain network, these policies allow for collaboration between workers who may be located in different parts of the world. By creating these policies and profiles the network administrator makes it one step harder for an unauthorised user the gain access to what they are not allowed to see.

1. Firewalls

A firewall is another form of security that can be used for a network. Firewalls block access to the network from outsiders as well as protecting confidential information. A firewall is a combination of hardware and software that will only allow authorised network traffic to pass through it.

1. Antivirus software

Antivirus software is used to prevent computer virus infections; it detects the presence of viruses as the computer boots up, when an executable is run, when documents are accessed or when files are copied. They can also detect viruses in files that have been downloaded from the internet. When this program finds a virus it may deal with it automatically or send a warning message to the user so they can take further action.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.

The security considerations for communication with an organisation are:

* Well-documented processes for communicating sensitive information via email, telephone and fax
* Use of passwords on documents that have sensitive information
* Well-documented policy for the use of networked devices within the organisation

**Storage**

1. **File naming conventions**
   1. List the 3 types of information each document should include.

The three types of information that each document should contain:

* Date stamp: a date that indicates the timeliness of a document. This should be different to the metadata saved with each file that indicates the date the file was created and when it was last saved.
* Variation: a label which identifies which version of the files is saved. For example v3.docx or document\_final.docx. This allows employees to keep track of which version they are working on.
* Name: Tho document should have a title that is meaningful and can easily identify the document.
  1. Give an example of a sequential file-naming convention.

An example of sequential file-naming system convention is ‘Newsletter 2011-11 03Oct.doc’. This is a monthly newsletter; the edition being prepared is for November 2011.

1. **Location of files-**
2. **Backups**
   1. Distinguish between each of the following:
      1. Full backup

Full backup copies all of the files from a device on a storage medium. It takes considerable time and is usually performed over time period such as a week, fortnight or month.

* + 1. Differential backup

A differential backup copies only the files that have been changed since the last full backup. Restoration of files would involve restoring the files from the full backup and then from the differential backup.

* + 1. Incremental backup

An incremental backup is similar to a differential backup, the difference being that it uses more than two backup media, while a differential backup only uses two. An incremental backup also only copies what has been changed since the last full backup. This method is the most complicated to restore files since it requires restoration from a full backup and then from a series of incremental backups.

1. **Backup timeline**
   1. List good practice in relation to backup timelines.

It is good practice to label all backup media so that you know when the backup was made and what it was on. Al log may also be kept of the by a systems manager recording the dates of backup, the location of files and whether or not any restorations have been made.

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

Ideally backup files should be stored in a located somewhere that is safe from theft and damage that can be caused by extreme temperatures or disasters. Backups may even be stores in a remote location or another city.

* 1. What is the grandparent-parent-child system?

The grandparent-parent-child system is a suggested backup routine. The parent is the second oldest copy of the file; the child is the newest copy of the file. For example the first backup file will be called the child, the second backup this file will be called the parent and the new file called the child, at the third backup the first file will be called the grandparent the second the parent and the most recent (third) backup will be called the child.

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

Archiving is the process if copy files to long-term then deleting them from the hard disk, whereas destruction involves deletion only.

* 1. What is a problem for ICT managers?

A problem for ICT managers is determining what the most appropriate long-term storage medium to use is. For example if the files are to be stored on a CD for several years the ICT manager has to ensure that the CD will not deteriorate and that there will still be CD-ROM drives around to read the CD.

* 1. What is a legacy system?

A legacy system is an old system. These systems are used to run old databases on old servers or main frames.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

When disposing of information organisations must consider protection sensitive data (there are currently many ways of ‘deleting’ data from a storage medium as none of them can completely guarantee that information is completely disposed of).

Darcie Anderson